**Мельник Віктор Анатолійович. Конфігуровані ядра комп'ютерних пристроїв симетричного блокового шифрування: дис... канд. техн. наук: 05.13.05 / Національний ун-т "Львівська політехніка". - Львів, 2004**

**Мельник В.А. Конфігуровані ядра комп’ютерних пристроїв симетричного блокового шифрування. – Рукопис.**

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – елементи та пристрої обчислювальної техніки та систем керування. – Національний університет “Львівська політехніка”, Львів, 2004.

Дисертація присвячена розробці принципів побудови конфігурованих ядер комп’ютерних пристроїв, розробці конфігурованих ядер комп’ютерних пристроїв симетричного блокового шифрування (СБШ), а також створенню на їх основі нових високопродуктивних та малогабаритних апаратно-орієнтованих процесорів СБШ, що відповідають вимогам широкого кола застосувань.

Досліджено принципи побудови алгоритмів СБШ, поширені алгоритми СБШ, режими шифрування, що в них використовуються, а також сучасні підходи до апаратної реалізації алгоритмів СБШ. Розглянуто технологію проектування комп’ютерних систем на кристалі на основі ядер програмованих та апаратно-орієнтованих комп’ютерних пристроїв, показано суттєві переваги останніх та доцільність їх застосування при реалізації алгоритмів СБШ. Вперше розроблено формалізовану конфігуровану модель комп’ютерного пристрою, на основі якої шляхом задання конфігураційних параметрів можна отримати модель комп’ютерного пристрою з заданими технічними характеристиками. Розроблено нові технології генерації ядер комп’ютерних пристроїв, які характеризуються високою гнучкістю і простотою реалізації. Досліджено задачу тестування генераторів ядер комп’ютерних пристроїв, виділено методи їх тестування та запропоновано структуру системи їх тестування. Розроблено принципи побудови та конфігуровані структури функціональних вузлів процесорів СБШ, структури функціональних вузлів процесорів СБШ за алгоритмами DES і Triple DES, на основі яких можна реалізувати повний ряд ядер цих процесорів. Проведено аналіз організації обчислень та режимів шифрування в алгоритмах СБШ DES і Triple DES, що дозволило виділити доцільні до реалізації типи процесорів СБШ, які виконують ці алгоритми. З використанням запропонованих технологій генерації ядер комп’ютерних пристроїв та сучасних засобів проектування реалізовано повний ряд ядер процесорів СБШ за алгоритмами DES і Triple DES.